Efficient Hardware for the Tate Pairing Calculation in Characteristic Three

T. Kerins[1], W.P. Marnane[1], E.M. Popovici[2] and P.S.L.M. Barreto[3]

[1] *Department of Electrical and Electronic Engineering,*
[2] *Department of Microelectronic Engineering,*
University College Cork, Ireland

[3] *Dept. Computing and Digital Systems Engineering, Escola Politécnica,*
Universidade de São Paulo, Brazil

Overview of Presentation

- Introduction and some related work
- The Modified Duursma-Lee algorithm in characteristic $p = 3$
- Tower-field arithmetic for Tate pairing calculation
- The advantage(s) of designing dedicated hardware for the Tate pairing calculation
- Some results and conclusions

Overview of Presentation

- Introduction and some related work
- The Modified Duursma-Lee algorithm in characteristic $p = 3$
- Tower-field arithmetic for Tate pairing calculation
- The advantage(s) of designing dedicated hardware for the Tate pairing calculation
- Some results and conclusions

Introduction

- In simple terms a pairing is a mapping from two points on an elliptic curve to an element of the underlying Galois field
- Pairings are an important development in constructive cryptography
- They allow the construction of protocols not readily available from other primitives, for example the Boneh-Franklin IBE scheme

The Tate pairing

- This work focuses on implementing the Tate pairing on *supersingular elliptic* curves

$$E_{\pm}(GF(3^m)) : y^2 = x^3 - x \pm 1$$

The Tate pairing

- This work focuses on implementing the Tate pairing on *supersingular elliptic* curves

$$E_{\pm}(GF(3^m)) : y^2 = x^3 - x \pm 1$$

- maximum *security multiplier* of $k = 6$

The Tate pairing

- This work focuses on implementing the Tate pairing on *supersingular elliptic* curves

$$E_{\pm}(GF(3^m)) : y^2 = x^3 - x \pm 1$$

  - maximum *security multiplier* of $k = 6$
  - efficiently implementable

The Tate pairing

- This work focuses on implementing the Tate pairing on *supersingular elliptic* curves

$$E_{\pm}(GF(3^m)) : y^2 = x^3 - x \pm 1$$

  - maximum *security multiplier* of $k = 6$
  - efficiently implementable
  - $GF(3^m)$ arithmetic architectures less well studied than $GF(2^m)$ and $GF(p)$

Recent History of Tate Pairing Calculation

- 1986 : Miller's Algorithm - double & add

Recent History of Tate Pairing Calculation

- 1986 : Miller's Algorithm - double & add
- 2002 : GHS Algorithm - triple & add

Recent History of Tate Pairing Calculation

- 1986 : Miller's Algorithm - double & add
- 2002 : GHS Algorithm - triple & add
- 2002 : BLKS Algorithm :*distortion map* and simpler line function evaluation

Recent History of Tate Pairing Calculation

- 1986 : Miller's Algorithm - double & add
- 2002 : GHS Algorithm - triple & add
- 2002 : BLKS Algorithm :*distortion map* and simpler line function evaluation
- 2003 : Duursma-Lee Algorithm : simpler structure, incorporation of distortion map into pairing

Recent History of Tate Pairing Calculation

- 1986 : Miller's Algorithm - double & add
- 2002 : GHS Algorithm - triple & add
- 2002 : BLKS Algorithm :*distortion map* and simpler line function evaluation
- 2003 : Duursma-Lee Algorithm : simpler structure, incorporation of distortion map into pairing
- 2004 : Kwon Algorithm : Modified Duursma-Lee, suitable for efficient implementation on dedicated hardware

The Tate Pairing in hardware

- There has been little published investigation into the hardware implementation aspects of the $p = 3$ Tate pairing in hardware ...
  - 2004 : Kerins, Marnane and Popovici
  - 2004 / 2005 : Granger Page and Stam
  - 2005 : This conference
  - 2005 : Kerins, Marnane Popovici and Barreto (IEE. Trans IT *to appear*)

Overview of Presentation

- Introduction and some related work
- The Modified Duursma-Lee algorithm in characteristic $p = 3$
- Tower-field arithmetic for Tate pairing calculation
- The advantage(s) of designing dedicated hardware for the Tate pairing calculation
- Some results and conclusions

Overview of Presentation

- Introduction and some related work
- The Modified Duursma-Lee algorithm in characteristic $p = 3$
- Tower-field arithmetic for Tate pairing calculation
- The advantage(s) of designing dedicated hardware for the Tate pairing calculation
- Some results and conclusions

The Modified Tate Pairing (char 3)

$$\begin{aligned} E_{\pm}(GF(3^m))[l] \times E_{\pm}(GF(3^m))[l] &\rightarrow GF(3^{6m})^* \\ \{P = (x_p, y_p)\} \times \{R = (x_r, y_r)\} &\rightarrow \tau \end{aligned}$$

$$\text{Modified Tate pairing : } \hat{e}(P, R) = \tau \in GF(3^{6m})^*$$

The Modified Tate Pairing (char 3)

$$\begin{array}{rcl} E_{\pm}(GF(3^m))[l] \times E_{\pm}(GF(3^m))[l] & \longrightarrow & GF(3^{6m})^* \\ \{P = (x_p, y_p)\} \times \{R = (x_r, y_r)\} & \longrightarrow & \tau \end{array}$$

$$\text{Modified Tate pairing : } \hat{e}(P, R) = \tau \in GF(3^{6m})^*$$

- $\hat{e}(P, R) = e_{e^{3m-1}}(P, \phi(R))^{\epsilon_T}$, where $\epsilon_T = 3^{3m-1}$

The Modified Tate Pairing (char 3)

$$\begin{array}{rcl} E_{\pm}(GF(3^m))[l] \times E_{\pm}(GF(3^m))[l] & \longrightarrow & GF(3^{6m})^* \\ \{P = (x_p, y_p)\} \times \{R = (x_r, y_r)\} & \longrightarrow & \tau \end{array}$$

Modified Tate pairing : $\hat{e}(P, R) = \tau \in GF(3^{6m})^*$

- $\hat{e}(P, R) = e_{e^{3m-1}}(P, \phi(R))^{\epsilon_T}$, where $\epsilon_T = 3^{3m-1}$
- $\phi : E_{\pm}(GF(3^m))[l] \longrightarrow E_{\pm}(GF(3^{6m}))[l]$
  $\phi(R) = (\rho - x_r, \sigma y_r)$

The Modified Tate Pairing (char 3)

$$\begin{aligned} E_{\pm}(GF(3^m))[l] \times E_{\pm}(GF(3^m))[l] &\rightarrow GF(3^{6m})^* \\ \{P = (x_p, y_p)\} \times \{R = (x_r, y_r)\} &\rightarrow \tau \end{aligned}$$

Modified Tate pairing : $\hat{e}(P, R) = \tau \in GF(3^{6m})^*$

- $\hat{e}(P, R) = e_{e^{3m-1}}(P, \phi(R))^{\epsilon_T}$, where $\epsilon_T = 3^{3m-1}$
- $\phi : E_{\pm}(GF(3^m))[l] \rightarrow E_{\pm}(GF(3^{6m}))[l]$
  $\phi(R) = (\rho - x_r, \sigma y_r)$
- $\rho^3 - \rho \mp 1 = 0$, $\sigma^2 + 1 = 0$, $\rho, \sigma \in GF(3^{6m})$

The Modified Duursma-Lee (Kwon) Algorithm

```
$\alpha = x_p, \beta = y_p, x = x_r^3, y = y_r^3,\ d = (\pm m) \bmod 3$
loop $m$ times
    $\alpha = \alpha^9, \beta = \beta^9$                 (* arith. in $GF(3^m)$ *)
    $\mu = \alpha + x + d$                               (* arith. in $GF(3^m)$ *)
    $\gamma = -\mu^2 - \beta y \sigma - \mu\rho - \rho^2$     (* arith. in $GF(3^{6m})$ *)
    $t = t^3$                                            (* cubing in $GF(3^{6m})$ *)
    $t = t * \gamma$                                     (* multiplication in $GF(3^{6m})$ *)
    $y = -y\ d = (d \mp 1) \bmod 3$                      (* arith. in $GF(3^m)$ *)
end loop and return $t$
```

Calculation of Modified Tate Pairing

- involves ...
  - calculation of $e_{3^{3m}-1}(P, \phi(R)) = t \in GF(3^{6m})$
  - exponentiation $\hat{e}(P, R) = t^{\epsilon_1} = \tau \in GF(3^{6m})$
- Kwon Algorithm is calculated using mainly
  - multiplication and cubing in $GF(3^m)$
  - multiplication and cubing in $GF(3^{6m})$
- Our contribution : these can be efficiently parallelized on dedicated hardware

Aim of this research

- How efficiently the modified Tate paring can be performed on dedicated hardware?
- Xilinx FPGA technology was chosen as implementation platform
- From this insight can be gained into issues related to and eventual ASIC implementation
- Application as a high performance server accelerator

Overview of Presentation

- Introduction and some related work
- The Modified Duursma-Lee algorithm in characteristic $p = 3$
- Tower-field arithmetic for Tate pairing calculation
- The advantage(s) of designing dedicated hardware for the Tate pairing calculation
- Some results and conclusions

Overview of Presentation

- Introduction and some related work
- The Modified Duursma-Lee algorithm in characteristic $p = 3$
- Tower-field arithmetic for Tate pairing calculation
- The advantage(s) of designing dedicated hardware for the Tate pairing calculation
- Some results and conclusions

Arithmetic in $GF(3^m)$ -1

- Polynomial basis arithmetic
- 2003 : Efficient digit serial multiplier architecture - Bertoni *et al.*
- Multiplication in $\lceil m/D \rceil$ clock cycles
- Dedicated cubing circuitry in single clock cycle
- Additive operations by simple gate circuits using a 2 bit encoding for elements of $GF(3)$

Representation of $GF(3^{6m})$ - 1

- This is the principal complexity in the implementation $\hat{e}(P, R)$
- Aim : to simplify this as much as possible ...
- Represent $GF(3^{6m})$ as an extension field of $GF(3^m)$
- 2004 : Choose the *tower field* representation defined by the distortion map ϕ - Granger / Page / Stam

Representation of $GF(3^{6m})$ -2

- $GF(3^{2m}) \cong GF(3^m)[\sigma]/\sigma^2 + 1$
- $GF(3^{6m}) \cong GF(3^{2m})[\rho]/\rho^3 - \rho \mp 1$

Representation of $GF(3^{6m})$ -2

- $GF(3^{2m}) \cong GF(3^m)[\sigma]/\sigma^2+1$
- $GF(3^{6m}) \cong GF(3^{2m})[\rho]/\rho^3-\rho\mp 1$
- elements of $GF(3^{6m})$ are represented as 6-tuples of $GF(3^{6m})$ elements, basis defined by

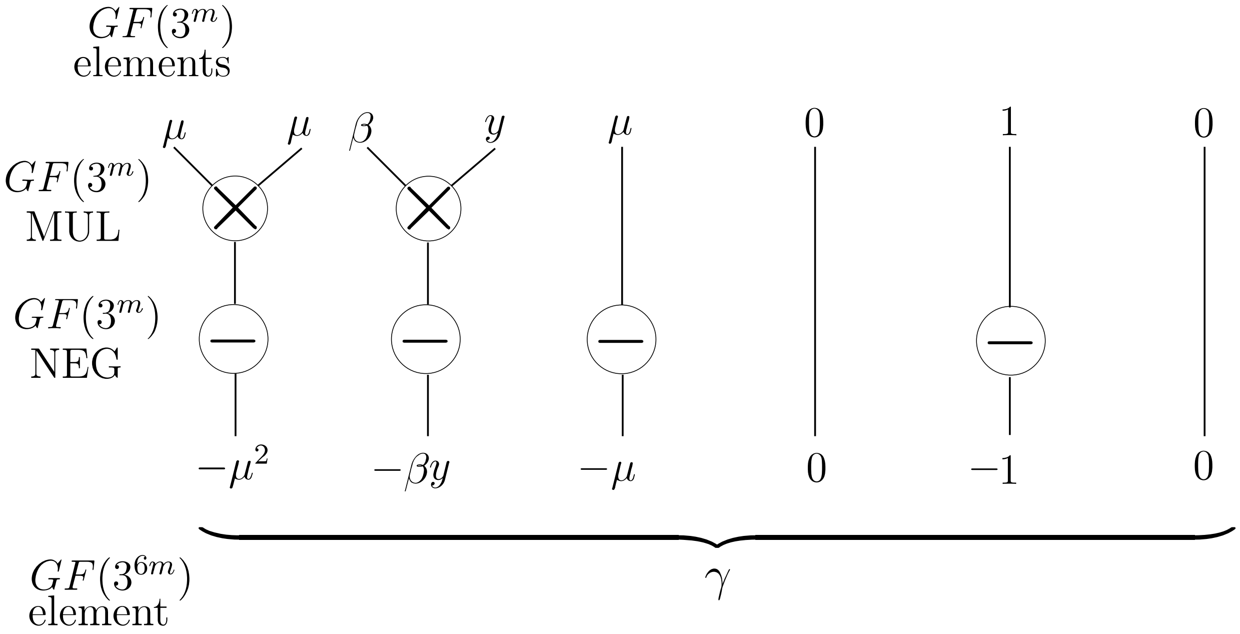
$$\{1, \sigma, \rho, \sigma\rho, \rho^2, \sigma\rho^2\}$$

- $GF(3^{6m})$ elements σ and ρ required in Step 05 of Kwon algorithm have simple representation

$$\sigma = [0,1,0,0,0,0] \qquad \rho = [0,0,1,0,0,0]$$

Efficient calculation of γ (Step 05)

- recall : $\gamma = -\mu^2 - \beta y \sigma - \mu\rho - \rho^2$



- requires only 2 $GF(3^m)$ multiplications, performed in parallel

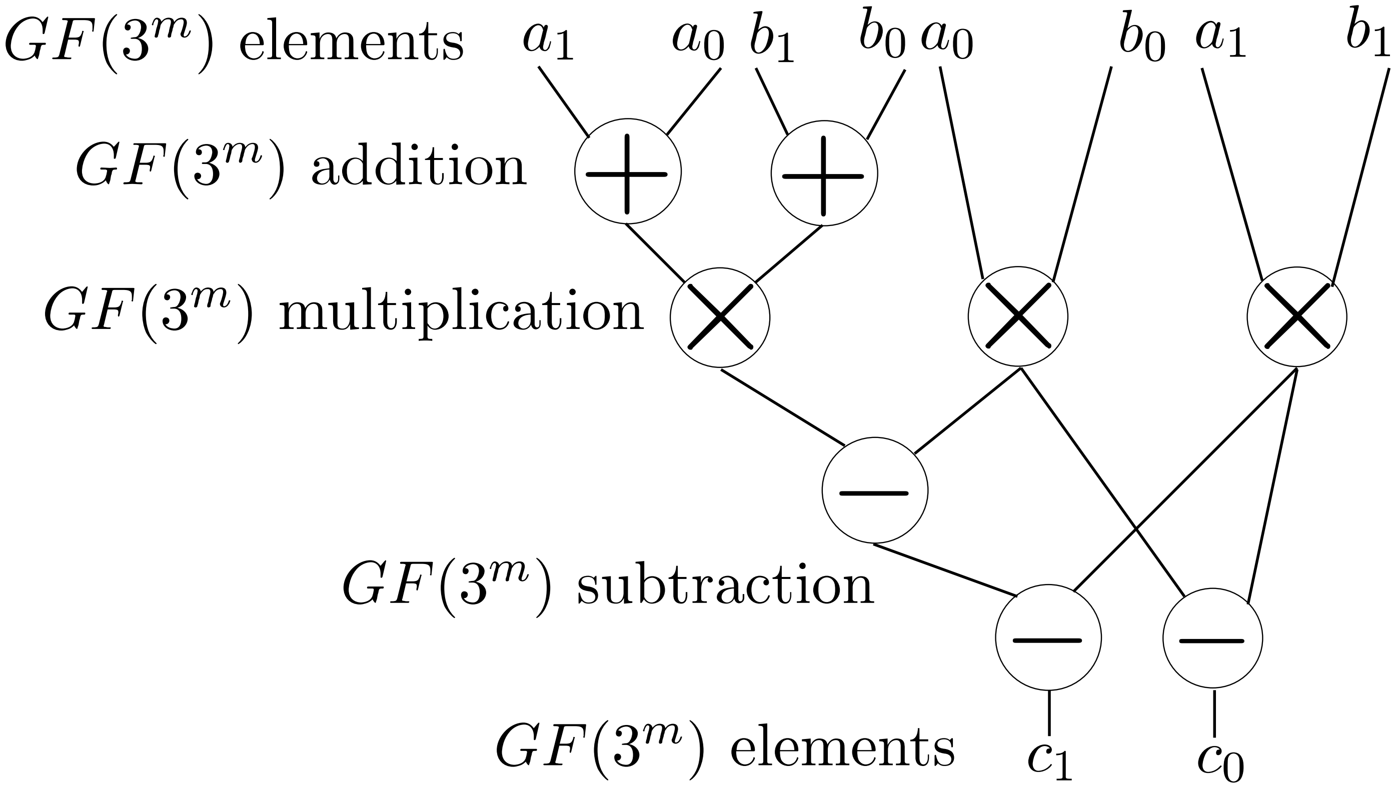
Multiplication in $GF(3^{2m})$ -1

- $\tilde{c} = \tilde{a}\tilde{b} \in GF(3^{2m})$, $\tilde{a} = a_1\sigma + a_0$, $\tilde{b} = b_1\sigma + b_0$
- Performed by *Karatsuba Multiplication*

$$\begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = \begin{bmatrix} a_0b_0 - a_1b_1 \\ (a_1 + a_0)(b_1 + b_0) - a_1b_1 - a_0b_0 \end{bmatrix}$$

- Requires three multiplications in $GF(3^m)$
- These multiplications can be performed in parallel

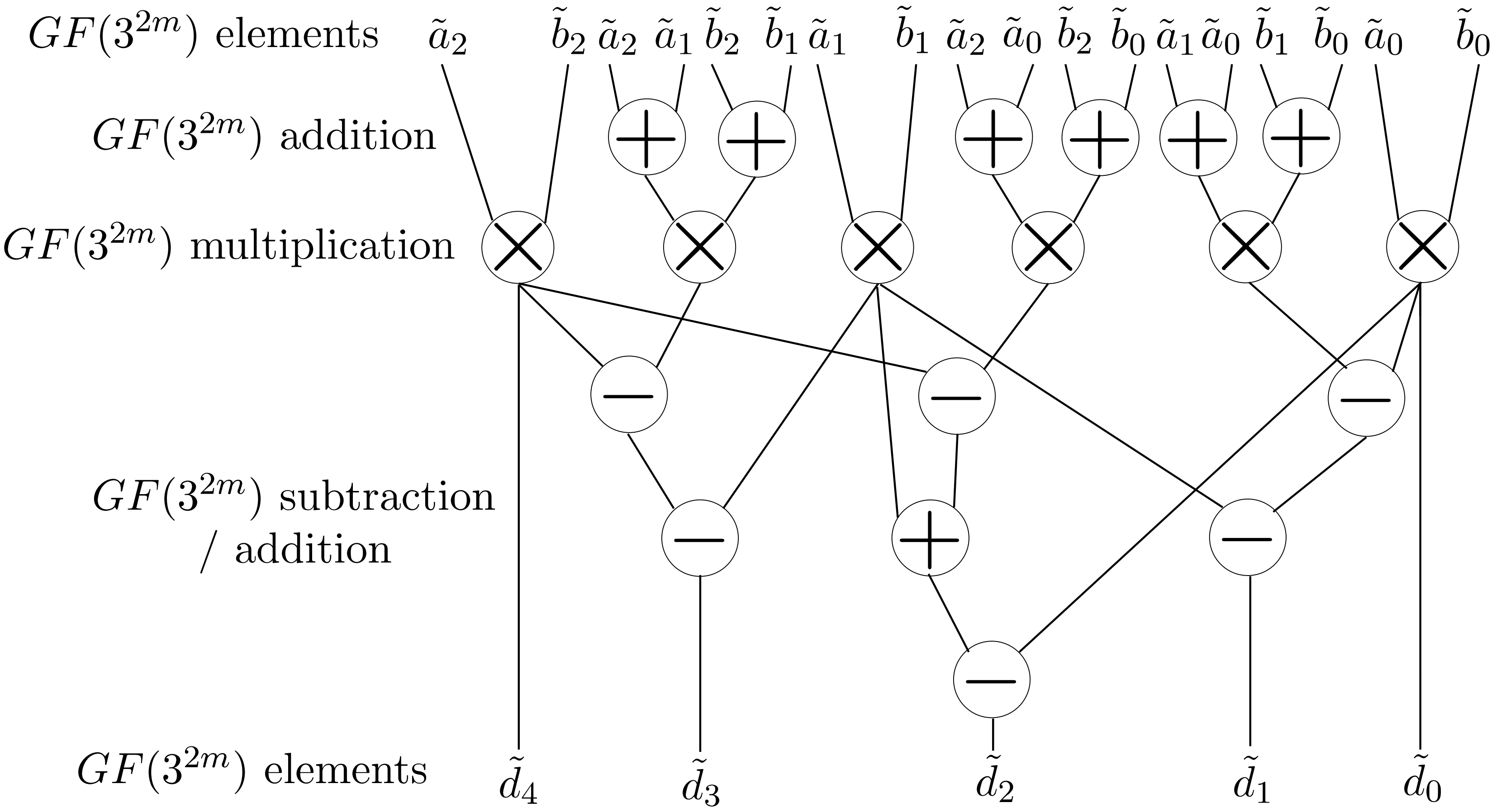
Multiplication in $GF(3^{2m})$ -2



Multiplication in $GF(3^{6m})$ -1

- $a \in GF(3^{6m}) : a = \underbrace{(a_0 + a_1\sigma)}_{\tilde{a}_0} + \underbrace{(a_2 + a_3\sigma)}_{\tilde{a}_1}\rho + \underbrace{(a_4 + a_5\sigma)}_{\tilde{a}_2}\rho^2$
- Multiplication in $GF(3^{6m})$ performed by multiplication of elements of $GF(3^{2m})$
- 2000 : Bailey / Paar method
- Requires 6 multiplications in $GF(3^{2m})$
- .. this implies 18 multiplications in $GF(3^m)$ required for arbitrary multiplication in $GF(3^{6m})$
- but all multiplications may be carried out in parallel

Multiplication in $GF(3^{6m})$ -2


$GF(3^{2m})$ elements
$\tilde{a}_2$ $\tilde{b}_2$ $\tilde{a}_2$ $\tilde{a}_1$ $\tilde{b}_2$ $\tilde{b}_1$ $\tilde{a}_1$ $\tilde{b}_1$ $\tilde{a}_2$ $\tilde{a}_0$ $\tilde{b}_2$ $\tilde{b}_0$ $\tilde{a}_1$ $\tilde{a}_0$ $\tilde{b}_1$ $\tilde{b}_0$ $\tilde{a}_0$ $\tilde{b}_0$
$GF(3^{2m})$ addition
$GF(3^{2m})$ multiplication
$GF(3^{2m})$ subtraction / addition
$GF(3^{2m})$ elements
$\tilde{d}_4$ $\tilde{d}_3$ $\tilde{d}_2$ $\tilde{d}_1$ $\tilde{d}_0$

Dataflow for composition stage of multiplication in $GF(3^{6m})$

Multiplication in $GF(3^{6m})$ -3

- Brought to out attention by Keith Harrison ...
- Some coefficients of γ from Kwon algorithm are guaranteed to be $0 \in GF(3^m)$
- Full multiplication in $GF(3^{6m})$ is in fact not required in Step 07 of Kwon algorithm
- ... in fact can be performed in 13 multiplications in $GF(3^m)$
- However it is interesting to consider the general case (18 multiplications) as this is also applicable to other Tate pairing algorithms

Cubing in $GF(3^{2m})$

- $\tilde{c} = c_0 + \sigma c_1 \in GF(3^{2m})$

$$\begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = \begin{bmatrix} a_0^3 \\ -a_1^3 \end{bmatrix}$$

- involves two cubing operations in $GF(3^m)$
- which may be performed in parallel

Cubing in $GF(3^{6m})$ -1

- Cubing in $GF(3^{6m})$ involves 3 cubing operations in $GF(3^{2m})$
- ... which implies that in total 6 cubing operations in $GF(3^m)$ are required
- as well as additive operations
- As these six cubing operations can be carried out in parallel
- and $GF(3^m)$ cubing can be performed in a single clock cycle
- Cubing in $GF(3^{6m})$ is possible in a single clock cycle

Raising to Tate Power $\epsilon_T = 3^{3m-1}$ -1

- The basis

$$\{1, \sigma, \rho, \rho\sigma, \rho^2, \sigma\rho^2\}$$

is converted to the other basis defined by ϕ

$$\{1, \rho, \rho^2, \sigma, \rho\sigma, \rho\sigma^2\}$$

by a simple rewiring in hardware

- Now $a \in GF(3^{6m})$

$$a = \underbrace{(a_0 + a_1\rho + a_2\rho^2)}_{\check{a}_0} + \underbrace{(a_3 + a_4\rho + a_5\rho^2)}_{\check{a}_1}\sigma$$

Raising to Tate Power $\epsilon_T = 3^{3m-1}$ -2

- $a^{3^{3m}} = (\check{a}_0 + \sigma\check{a}_1)^{3^{3m}} = \check{a}_0 - \sigma\check{a}_1$ for m odd as $\sigma = \sqrt{-1}$
- so ...

$$a^{\epsilon_T} = \frac{\check{a}_0 - \sigma\check{a}_1}{\check{a}_0 + \sigma\check{a}_1} = \left[1 + \check{a}_1^2\nu^{-1}\right] + \sigma\left[1 - (\check{a}_0 + \check{a}_1)^2\nu^{-1}\right]$$

where $\nu = (\check{a}_0^2 + \check{a}_1^2)$

- involves 5 multiplications in $GF(3^{3m})$
- Inversion in $GF(3^{3m})$ requires only a single inversion in $GF(3^m)$ and a number of multiplications
- 2004 : Inverter circuit for $GF(3^m)$ - Kerins *et al.*

Overview of Presentation

- Introduction and some related work
- The Modified Duursma-Lee algorithm in characteristic $p = 3$
- Tower-field arithmetic for Tate pairing calculation
- The advantage(s) of designing dedicated hardware for the Tate pairing calculation
- Some results and conclusions

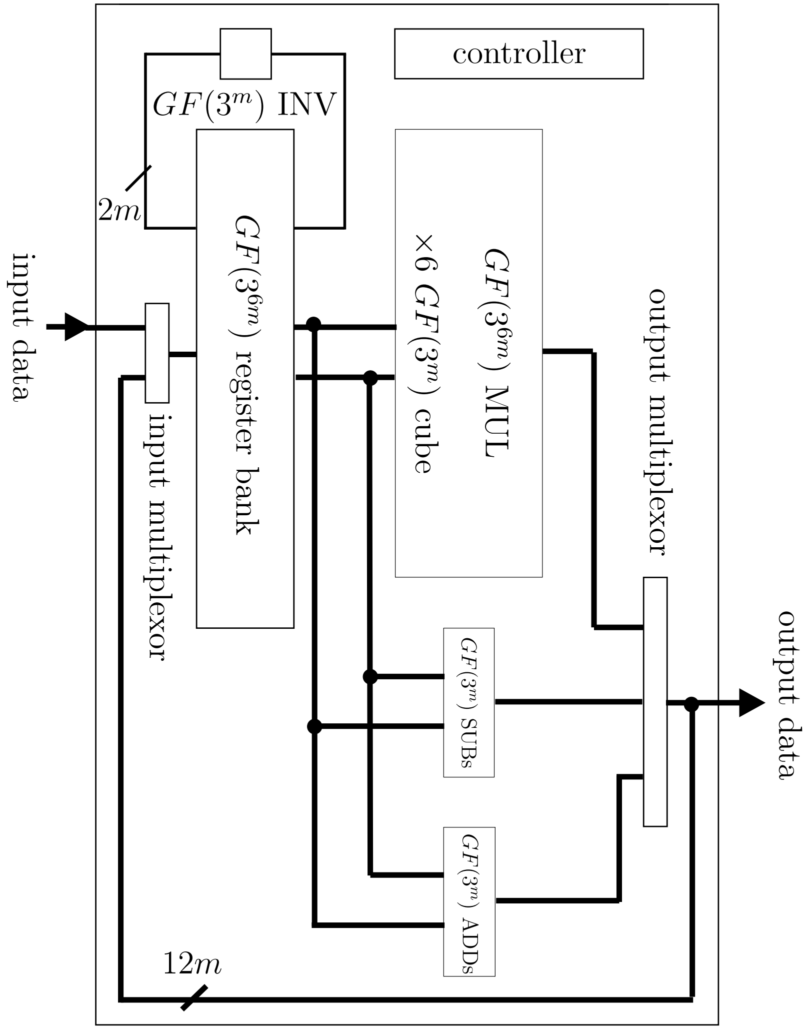
Overview of Presentation

- Introduction and some related work
- The Modified Duursma-Lee algorithm in characteristic $p = 3$
- Tower-field arithmetic for Tate pairing calculation
- The advantage(s) of designing dedicated hardware for the Tate pairing calculation
- Some results and conclusions

A Hardware Architecture -1

- Consider number of clock cycles required for each iteration of the Kwon algorithm
- Assume eighteen $GF(3^m)$ digit serial multipliers (digit size D, calculation in $d = \lceil m/D \rceil$ clock cycles)
- and also six $GF(3^m)$ cubing circuits (calculation in a single clock cycle) are available in parallel
- Also $2m$ bit registers for storage of elements of $GF(3^m)$ and $12m$ bit data lines for propagation of elements of $GF(3^{6m})$
- and simple gate circuitry for additive operations

A Hardware Architecture -2



Clock cycles for iteration of Kwon Algorithm

Step	operations	$GF(3^m)$ logic	clock cycles
03	$\alpha = \alpha^9$, $\beta = \beta^9$	×4 cube	2+2
04	$\mu = \alpha + x + d$	combinational	0+2
05	γ	×2 mul	$d + 2$
06	$t = t^3$	×6 cube	$1 + 2$
07	$t = t\gamma$	×18 mul	d+n_m+2
08 09	$y = -y$, $d = d \mp 1$	combinational	0+2

Calculation time for $\hat{e}(P, R)$ on this Architecture

- Kwon Algorithm : $e_{3^{3m-1}}(P, \phi(R)) = t \in GF(3^{6m})$

$$m(\lceil m/D \rceil + 17 + n_m) \text{ clock cycles}$$

- Raising to Tate power : $\hat{e}(P, R) = \tau = t^{\epsilon_T}$

$$9(\lceil m/D \rceil + n_m) + 2m \text{ clock cycles}$$

- Assume (worst case) that $n_m \approx \lceil m/D \rceil$ to get a calculation time of

$$\underline{3m(\lceil m/D \rceil + 17) + 18\lceil m/D \rceil + 2m}$$

Overview of Presentation

- Introduction and some related work
- The Modified Duursma-Lee algorithm in characteristic $p = 3$
- Tower-field arithmetic for Tate pairing calculation
- The advantage(s) of designing dedicated hardware for the Tate pairing calculation
- Some results and conclusions

Overview of Presentation

- Introduction and some related work
- The Modified Duursma-Lee algorithm in characteristic $p = 3$
- Tower-field arithmetic for Tate pairing calculation
- The advantage(s) of designing dedicated hardware for the Tate pairing calculation
- Some results and conclusions

Implementation Aspects of $GF(3^m)$ Arithmetic

- How practical is an architecture with eighteen $GF(3^m)$ multiplier circuits?
- On the Xilinx Virtex2Pro125 device designed for the field $GF(3^{97})/x^{97}+x^{16}+1$
  - $D = 4$ multiplier architecture (multiplication in 25 clock cycles) occupies 1,821 FPGA slices (3 %)
  - cubing circuit (single clock cycle) occupies 314 FPGA slices (0.5 %)

$GF(3^{6m})$ Multiplier Architecture

- Most complex part of the proposed architecture
- Occupies 32,403 FPGA slices including routing (58 %)
- $m = 97$, multiplication in 25 clock cycles
- Post place-and-route frequency 29.3 MHz
- Multiplication time of 0.9 μs

$GF(3^{97})$ Tate Pairing Architecture

- Remaining 40 % of device can easily accommodate the remaining logic
- Using $D = 4$ the calculation of $\hat{e}(P, R)$ can be performed in 12,866 clock cycles
- Assuming a conservative 15 MHz for entire architecture
- ... $\underline{\hat{e}(P, R)\text{ calculation in }0.85\ ms}$
- Recent software implementations have reported $> 4\ ms$ for same calculation

Conclusions

- Modified Tate pairing can accelerated on dedicated hardware
- Improvement over software on serial general purpose processors
- Modern FPGAs are capable of accommodating such parallel architectures
- With changes in control hardware can be reused to accelerate other operations in pairing based protocols
- Even higher performance is possible on other technologies ...???

Thank You

Questions?

timk@rennes.ucc.ie liam@rennes.ucc.ie